



2131

Please type a plus sign (+) inside this box → ☐

PTO/SB/21 (08-00)
Approved for use through 10/31/2002. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM <i>(to be used for all correspondence after initial filing)</i>	Application Number	09/682, >56	
	Filing Date	08/10/2001	
	First Named Inventor	Ta-Kuang Yang	
	Group Art Unit	2131	
	Examiner Name		
Total Number of Pages in This Submission		Attorney Docket Number	MSV001

ENCLOSURES (check all that apply)		
<input type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Assignment Papers (for an Application)	<input type="checkbox"/> After Allowance Communication to Group
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input type="checkbox"/> Amendment / Reply	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address	<input type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Terminal Disclaimer	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> Request for Refund	
<input checked="" type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Response to Missing Parts/Incomplete Application	Remarks	
<input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53		

RECEIVED
SEP 24 2001
Technology Center 2100

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Firm or Individual name	WINSTON HSU
Signature	Winston Hsu
Date	9/14/2001

CERTIFICATE OF MAILING			
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, Washington, DC 20231 on this date: <input type="text"/>			
Typed or printed name			
Signature		Date	

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

11


+

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Supplemental Priority Data Sheet

Additional foreign applications:

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES NO
089116219	Taiwan, R.O.C.	08/11/2000	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> YES <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>



RECEIVED
SEP 24 2001
Technology Center 2100

Additional provisional applications: _____

Application Number	Filing Date (MM/DD/YYYY)

Additional U.S. applications:

U.S. Parent Application Number	PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

+



Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2001

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT

(\$)

0

Complete if Known

Application Number	09/682,256
Filing Date	08/10/2001
First Named Inventor	Ta-Kuang Yang
Examiner Name	
Group Art Unit	2/31
Attorney Docket No.	MSV001

METHOD OF PAYMENT

1. ☐ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:
- Deposit Account Number: 50-0801
- Deposit Account Name: North America International Patent Office
- ☒ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17
- ☐ Applicant claims small entity status. See 37 CFR 1.27
2. ☐ Payment Enclosed:
- ☐ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code (\$)	Fee Code (\$)	Fee Code (\$)	Fee Code (\$)		
101	710	201	355	Utility filing fee	
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) (\$)

0

2. EXTRA CLAIM FEES

	Extra Claims	Fee from below	Fee Paid
Total Claims	-20** =	X	
Independent Claims	-3** =	X	
Multiple Dependent			

Large Entity		Small Entity		Fee Description
Fee Code (\$)	Fee Code (\$)	Fee Code (\$)	Fee Code (\$)	
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2)

(\$)

0

**or number previously paid, if greater. For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code (\$)	Fee Code (\$)	Fee Code (\$)	Fee Code (\$)		
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for ex parte reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application*	

Other fee (specify) _____

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$)

0

SUBMITTED BY

Name (Print/Type)

WINSTON HSU

Registration No.
(Attorney/Agent)

41,526

Complete (if applicable)

Telephone

886-2-8923-7350

Signature

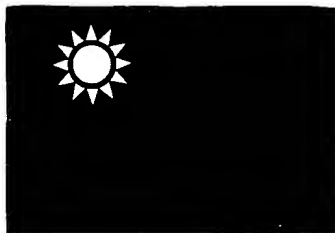
Winston Hsu

Date

9/15/2001

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下：

This is to certify that annexed is a true copy from the records of this
office of the application as originally filed which is identified hereunder:

申請日：西元 2000 年 08 月 11 日
Application Date

申請案號：089116219
Application No.

申請人：優碩資訊科技股份有限公司
Applicant(s)

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

RECEIVED
SEP 24 2001
Technology Center 2100

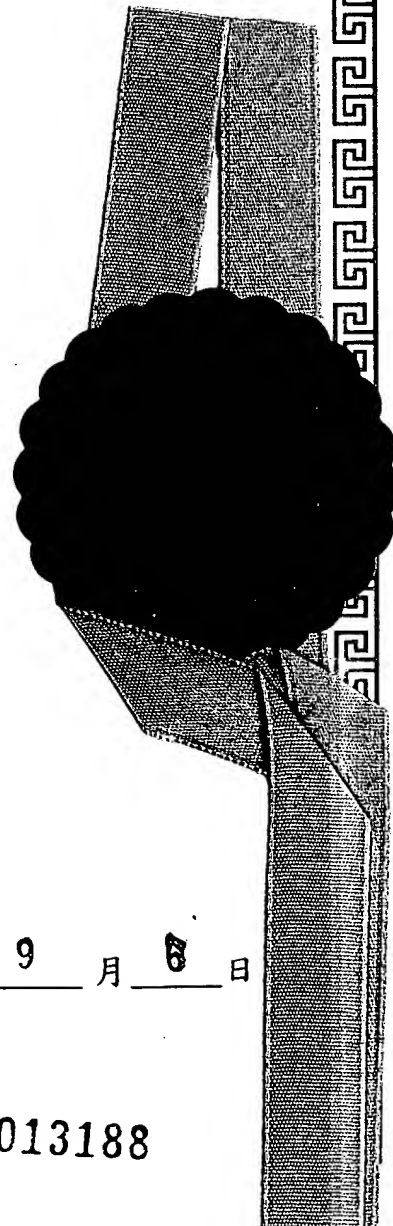
局長
Director General

陳明邦

發文日期：西元 2001 年 9 月 8 日
Issue Date

發文字號：
Serial No.

09011013188



申請日期：

案號：

類別：

(以上各欄由本局填註)

發明專利說明書

可防止電子文件盜拷之方法及其系統

中文

發明名稱

英文

1. 楊大廣

姓名
(中文)

1. Ta-Kuang Yang

姓名
(英文)

發明人

國籍

1. 中華民國

1. 台北市士林區克強路10巷3弄2號

住、居所

姓名
(名稱)
(中文)

1. 優碩資訊科技股份有限公司

姓名
(名稱)
(英文)

1. Neovue Inc.

國籍

1. 中華民國

住、居所
(事務所)

1. 台北市衡陽路10號13樓

代表人
姓名
(中文)

1. 戴英杰

代表人
姓名
(英文)

1.

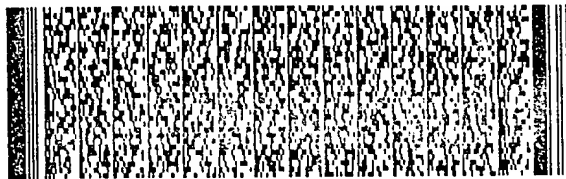
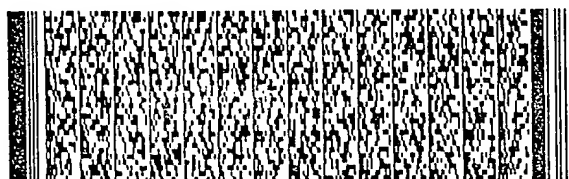


四、中文發明摘要 (發明之名稱：可防止電子文件盜拷之方法及其系統)

本發明係提供一種使用於電腦系統中的方法，以防止電子文件盜拷的情形產生。該電腦系統包含有一伺服器主機可經由一網際網路以與複數個終端機相連接，每一終端機並具有至少一代表該終端機之電腦辨識碼，該方法包含有步驟：(一)使用者載入一閱讀應用程式於一終端機中，該閱讀應用程式並包含一第一加密鑰匙；(二)使用者利用該閱讀應用程式向該伺服器主機註冊成為一合法之終端機，該伺服器主機並因此取得相關之使用者資料；(三)該伺服器主機在完成該終端機之合法註冊後，會產生一使用者辨識碼與一使用者專屬之第二加密鑰匙，該使用者辨識碼與該第二加密鑰匙並會以第一加密鑰匙經過加密後傳送至該

英文發明摘要 (發明之名稱：)

合法註冊之終端機；(四)該終端機之閱讀應用程式並會進一步將接收到之使用者辨識碼與第二加密鑰匙連同代表該終端機之電腦辨識碼一併加密以形成一終端機加密檔，以儲存於該合法註冊之終端機中。該文件索取程序包含有下列步驟：(一)當一終端機向該伺服器主機提出索取一電子文件之要求時，該伺服器主機則會將該電子文件之明文經過該第二加密鑰匙之加密而形成相對應之密文，並將該密文經由該網際網路傳送至該終端機；(二)當該終端機之閱讀應用程式接收到該密文時，會先以該第一加密鑰匙對該終端機加密檔解密，並取得其中之第二加密鑰匙與電腦



四、中文發明摘要 (發明之名稱：可防止電子文件盜拷之方法及其系統)

辨識碼；以及(三)當該閱讀應用程式比較所取得之電腦辨識碼與目前終端機之電腦辨識碼為相同時，即以該第二加密鑰匙對該接收到的密文解密，否則即停止後續之解密動作，以防止非合法之終端機對該電子文件之盜拷。

英文發明摘要 (發明之名稱：)



本案已向

國(地區)申請專利

申請日期

案號

主張優先權



無

有關微生物已寄存於

寄存日期

寄存號碼

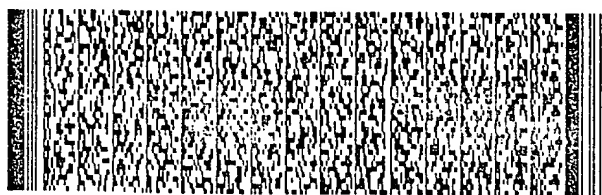
無

五、發明說明 (1)

本發明係提供一種使用於電腦系統中可防止電子文件盜拷的方法，尤指一種可防止利用網際網路下載電子文件至一電子閱讀裝置，卻又非法拷貝至其他電子閱讀裝置的方法。

傳統上知識是靠印刷於紙張上的書籍或雜誌來加以傳播，廣播及電視興起後加快了知識傳播的速度，如今電腦通訊及網際網路的蓬勃發展，更以驚人的速度將知識與資訊傳播到世界的各個角落。由於網際網路技術的發展，創造出許多新的商業模式，這些新的商業模式有一個共同的特點，就是利用網際網路來做生意，也就是近來通稱的電子商務。舉例而言，傳統上如果要購買書籍必須親自或請人到書店尋找後加以購買，由於網際網路的興起，如AMAZON等網路書店可以讓使用者在線上搜尋到想要的書籍並可直接下單購買。雖然，這使得購買書籍的方式大為簡化，然而，這還是一個不方便之處，就是有關書籍的保存，一但書籍購買的愈多愈需要足夠的空間來加以放置，同時管理上也更加繁雜。

有鑑於此，「電子閱讀裝置」的概念遂被提出以因應此種需要，也就是說將原來書籍中的文字或圖片數位化，形成電子書籍，消費者只要有一台終端機可以連接上網，再加上某些特定的程式軟體，就可以很方便地於線上購買想要的電子書籍或文件，並將此電子書籍下傳到消費者所

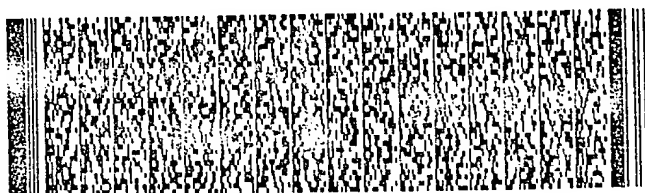
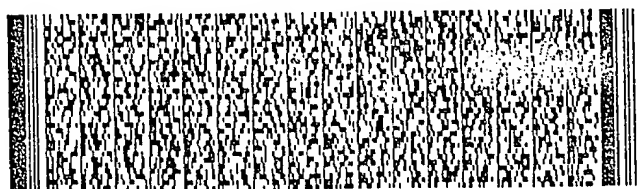


五、發明說明 (3)

子商務自然無法生存，這也就是電子書籍至今推展及普及的速度不如預期的重要原因。然而，電子書籍具有無紙化符合環保概念、效率化傳播速度的快速、經濟化不佔大量空間等多重優點，可節省許多珍貴的資源，如果只是因为未能解決上述「合法購買卻非法散佈」的情事而無法加以推廣，實在是經濟利益的重大損失。

有鑑於上述問題，本發明的主要目的是在提供一種使用於電腦系統中可防止電子文件盜拷的方法，尤指一種可防止利用網際網路下載電子文件至一電子閱讀裝置，卻又無法拷貝至其他電子閱讀裝置的方法，以解決上述問題。

請參閱圖一，圖一為本發明可防止電子文件盜拷之電腦系統之示意圖。本發明防盜拷電腦系統 100 包含有一伺服器主機 102 可經由一防火牆裝置 103 以連接上網際網路 104，另有複數個使用戶者也可經由各自的終端機 106、108、110 連接上網際網路 104。防火牆裝置 103 可用來區隔伺服器主機 102 與其外部的網際網路 104，其可透過網路訊息封包的過濾以及安全策略的訂定，讓某些特定的網路服務及安全的網路訊息，例如：經過註冊的遠端登錄、電子文件、檔案傳輸等可以進出防火牆裝置 103，以確保伺服器主機 102 中的設定及資訊不會遭受非法入侵及修改。每一終端機 106、108、110 可為一個人桌上型電腦 (desktop computer)、筆記型電腦 (notebook computer)、個人數位



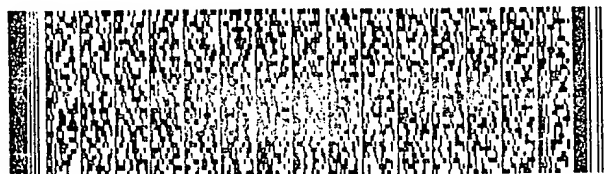
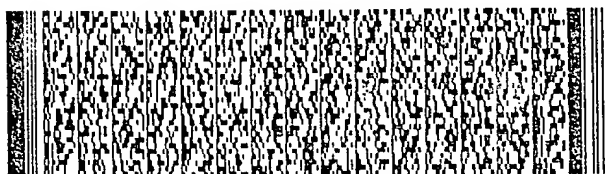
五、發明說明 (4)

助理器 (PDA)或是可連接上網的行動電話 (WAP cellular phone)等，只要用戶的終端機是可以連接上網並且傳輸數位資訊的都可以適用於本發明防盜拷電腦系統 100。

以本發明之較佳實施例而言，終端機 106、108、110 為個人桌上型電腦，其中包含一中央處理器，一硬碟機，一網路卡，輸入裝置如鍵盤、滑鼠、搖桿等，輸出裝置如螢幕、印表機等。每一終端機 106、108、110 中並各自具有至少一電腦辨識碼，用來代表終端機之身分認證，如中央處理器之辨識碼、硬碟機之辨識碼或是網路卡之辨識碼皆可成為該終端機之電腦辨識碼，以便伺服器主機 102 於後續電子交易或資料傳輸時可以確定各終端機 106、108、110 之身份或位置。

請參閱圖二，圖二為本發明防盜拷電腦系統之伺服器主機的功能方塊圖。伺服器主機 102 包含一介面模組 210，一公用程式模組 220，一註冊模組 230，一加密鑰匙產生模組 240，一加密模組 250，一交易處理及查證模組 260，一資料庫 270，與一控制中心 280。

伺服器主機 102 經由介面模組 210 與防火牆裝置 103 相連接，並透過防火牆裝置 103 與網際網路 104 進行資料傳輸與交換，並於必要時對不同規格的資料作適當的資料轉換。公用程式模組 220 中存放有伺服器主機 102 對外開放的

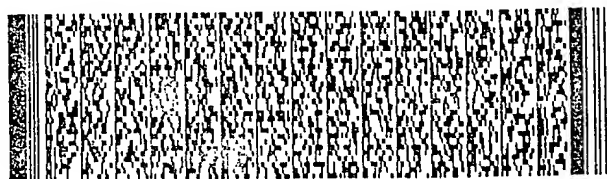


五、發明說明 (5)

各種公用程式，以供使用者免費下載至各自的終端機中，其中例如一經過編譯的閱讀應用程式，以提供使用者一登錄、註冊、下載、閱讀電子書籍的使用者操作介面，閱讀應用程式中並附加有一第一加密鑰匙，其功用容後再加詳述。註冊模組 230 則可接受使用者及其所指定的終端機之註冊，以便讓使用者成為合法登錄的使用者，而其所指定的終端機也成為合法登錄而可合法下載電子書籍的用戶終端機。加密鑰匙產生模組 240 會於使用者進行註冊時產生使用者專屬的第二加密鑰匙，也就是說不同的使用者其第二加密鑰匙都不相同。在此需加以說明，上述之第一及第二加密鑰匙其實就是一組預定長度的數位位元，例如可以是常用的 56 bits 或 128 bits，本發明之較佳實施例之鑰匙長度是採用 128 bits 或是更高的 bits，以增強其安全性。

加密模組 250 則是用來執行各種需要加密的動作，例如：於文件索取程序時，加密模組 250 會以使用者專屬的第二加密鑰匙對使用者購買的電子書籍加密以便後續傳送給使用者。交易處理及查證模組 260 則用來處理與使用者訂單有關的事宜，並對訂單的來源及內容進行必要的確認查證工作。

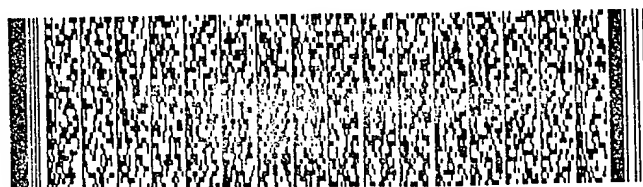
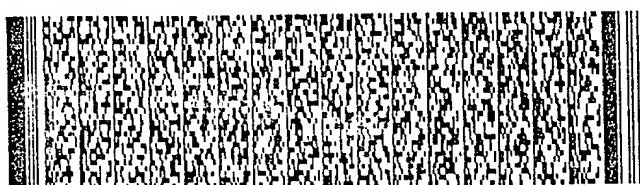
資料庫 270 則包含至少有三個子資料庫：用戶資料庫 272、密碼資料庫 274、電子文件資料庫 276。用戶資料庫



五、發明說明 (6)

272中存放有經過合法註冊後所有使用者相關的基本資料及其所指定的終端機的基本資料，如：代表某一用戶之使用者識別碼。密碼資料庫 274則存放使用者識別碼及其專屬的第二加密鑰匙之間的對照表，也就是說，每一個使用者在進行註冊時，加密鑰匙產生模組 240所產生相對應的專屬第二加密鑰匙就是存放在密碼資料庫 274中。電子文件資料庫 276則是存放將來要提供給讀者的電子書籍的明文，每一本電子書籍則有一獨特的電子書碼以方便查詢與建檔之用。而控制中心 280則是用來控制伺服器主機 102的操作，以及處理伺服器主機 102中各個模組或資料庫之控制或資訊流向。

請參閱圖三，圖三為本發明防盜拷電腦系統之終端機的功能方塊圖。以終端機 106為例，本發明終端機 106之較佳實施例為個人桌上型電腦，其中包含一中央處理器 302，一記憶體 320，一硬碟機 304，一網路卡 306，輸入裝置如鍵盤 308、滑鼠 310、搖桿 312等，輸出裝置如螢幕 314、印表機 316等。為了能與伺服器主機 102進行資料交換，終端機 106必須從伺服器主機 102之公用程式模組 220或網際網路 104上下載經過編譯的閱讀應用程式 322至終端機 106之記憶體 320或硬碟機 304中儲存。閱讀應用程式 322提供了使用者一登錄、註冊、下載、閱讀電子書籍的操作介面，其中並附加有第一加密鑰匙 324可供後續對終端機加密檔 326進行解密。即使是對於不同使用者而言，其所



五、發明說明 (7)

需要的閱讀應用程式 322 都是相同，因此閱讀應用程式 322 是事先經過編譯完成，並可供所有需要的使用者免費任意下載，而其中的第一加密鑰匙 324 也不因使用者的不同而有所區別。

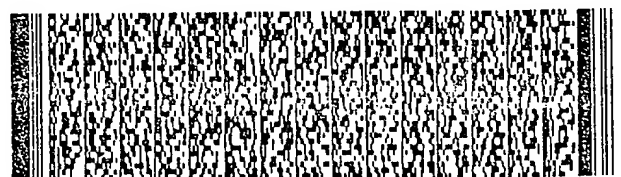
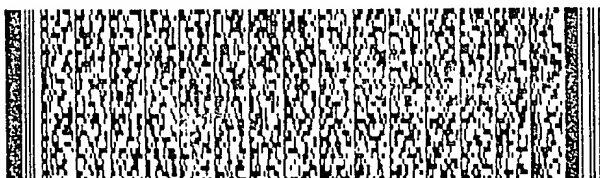
使用者以終端機 106 之閱讀應用程式為界面向遠端的伺服器主機 102 進行登錄與註冊時，其程序包括 1) 伺服器主機 102 辨識閱讀應用程式是否為合法的閱讀應用程式。 2) 伺服器主機 102 運用註冊模組 230 產生使用者識別碼與加密鑰匙產生模組 240 產生其相對應之第二加密鑰匙。 3) 伺服器主機 102 將使用者識別碼加入用戶資料庫 272 及第二加密鑰匙加入密碼資料庫 274。 4) 終端機 106 之閱讀應用程式下載使用者識別碼及第二加密鑰匙。每一終端機 106、108、110 於註冊完成後，會產生終端機加密檔 326，終端機加密檔 326 中包含有使用者識別碼 327、使用者之專屬第二加密鑰匙 328 與本台終端機 106 之電腦辨識碼 330，終端機 106 將終端機加密檔 326 以第一加密鑰匙 324 進行加密，並以加密的形式儲存於終端機 106 之記憶體 320 或硬碟機 304 中，以避免使用者不小心更改其中的內容，也可以減低其他人以非法的方式查看並得知其中的內容。當電子書籍下載後並需要進行解密之時，閱讀應用程式 322 會對終端機加密檔 326 以第一加密鑰匙 324 進行解密，以擷取出其中的第二加密鑰匙 328 與電腦辨識碼 330。



五、發明說明 (8)

現在針對本發明之方法作一詳細說明，配合本發明防盜拷電腦系統 100 之方法包含有一註冊程序與一文件索取程序。當一使用者想要利用本發明之電腦系統 100 進行電子書籍的購買之前，首先要從伺服器主機 102 或網際網路 104 上的網路書店下載閱讀應用程式 322，並於閱讀應用程式 322 中向伺服器主機 102 執行一註冊程序以成為一合法登錄的使用者或是會員，閱讀應用程式 322 中除了包含一般性的介面應用程式之外，還包含上述之第一加密鑰匙 324。在註冊的同時，不但使用者需要經過註冊，使用者將來所欲下載電子書籍的終端機 106 也需要經過註冊，也是說在註冊的過程中，相關之使用者基本資料（包括使用者辨識碼和其相對應的第二加密鑰匙 328）會經過註冊而儲存在伺服器主機 102 中。而使用者也必須以註冊當時所使用的終端機 106 作為將來下載電子書籍的電子閱讀裝置，否則，電腦系統 100 會判定所使用來下載電子書籍的電子閱讀裝置未經過註冊，而無法正常開啟所下載的電子書籍。

當使用者利用終端機 106 中的閱讀應用程式 322 進行註冊時，伺服器主機 102 會將使用者辨識碼儲存於用戶資料 272 中，然後指定一專屬的第二加密鑰匙 328 給使用者，並且將使用者與其第二加密鑰匙 328 之間的一對一對照關係儲存於密碼資料庫 274 中，如此便完成了使用者及其終端機 106 的合法註冊。在完成註冊後，伺服器主機 102 會以



五、發明說明 (9)

第一加密鑰匙將使用者辨識碼 327 與相對應該使用者之專屬第二加密鑰匙 328 加密，並傳送至終端機 106，而終端機之閱讀應用程式在接收到加密後的使用者辨識碼 327 與第二加密鑰匙 328 後，會先以第一加密鑰匙將兩者進行解密，而後進一步將解密後之使用者辨識碼與第二加密鑰匙連同代表該終端機之電腦辨識碼再一併加密以形成一終端機加密檔 326，並儲存於該合法註冊之終端機中，經過此一註冊程序，以後終端機 106 就可合法下載電子書籍並對其正確解密了。

請參閱圖四，圖四為本發明防盜拷電腦系統於註冊程序時之流程圖。將上述註冊程序以流程圖 400 表示如下列步驟：

步驟 402：開始；

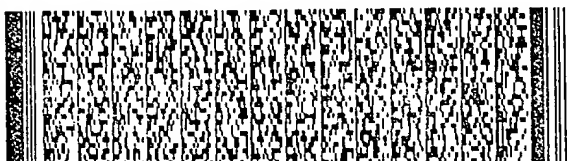
步驟 404：使用者選定一終端機 106 以進行後續註冊程序；

步驟 406：從網際網路 104 上下載閱讀應用程式 322 到選定的終端機 106；

步驟 408：由終端機 106 的閱讀應用程式 322 連接伺服器主機 102 進行註冊；

步驟 410：伺服器主機 102 產生使用者辨識碼及專屬的第二加密鑰匙 328 並分別儲存於用戶資料庫 272 與密碼資料庫 274 中；

步驟 412：伺服器主機 102 將產生的使用者辨識碼 327



五、發明說明 (10)

及其專屬的第二加密鑰匙 328 以第一加密鑰匙 324 加密後傳送至終端機 106；

步驟 414：終端機 106 之閱讀應用程式以第一加密鑰匙將接收到加密的使用者辨識碼 327 與第二加密鑰匙 328 進行解密；

步驟 416：終端機 106 之閱讀應用程式將解密後之使用者辨識碼 327 與第二加密鑰匙 328 連同代表終端機 106 之電腦辨識碼 330 再一併加密以形成一終端機加密檔 326；

步驟 418：終端機 106 之閱讀應用程式將終端機加密檔 326 儲存於其硬碟中；

步驟 420：結束。

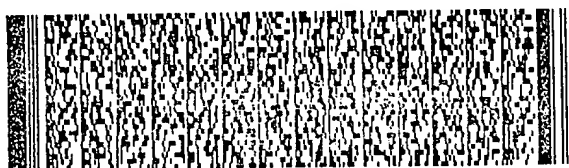
當使用者及其終端機 106 於伺服器主機 102 端完成註冊後，就可以依其個人意願於任何時候上網付費購買特定的電子書籍，並且將其下載至終端機 106，這一部份也就是本發明方法所稱之文件索取程序。使用者可從經過註冊之終端機於網際網路 104 中瀏覽網路書店或相關網站，進行搜尋並且決定購買某一本電子書籍，而將購買訂單傳送至伺服器主機 102，伺服器主機 102 在進行必要的確認及查證後，會於電子文件資料庫 276 中調出使用者想購買的電子書籍的明文，並且於密碼資料庫 274 中調出使用者專屬之第二加密鑰匙 328，之後以此第二加密鑰匙 328 對電子書籍的明文加密而形成相對應之密文，再將密文經由網際網路 104 傳送至終端機 106。



五、發明說明 (11)

當終端機 106 之閱讀應用程式 322 接收到所購買電子書籍的密文時，會先以閱讀應用程式 322 中附屬的第一加密鑰匙 324 對終端機加密檔 326 解密，以取得其中之第二加密鑰匙 328 與電腦辨識碼 330，然後閱讀應用程式 322 會對解密所取得之電腦辨識碼 330 與目前終端機 106 之電腦辨識碼 318 進行比對。當比對結果相同時，代表目前終端機 106 為經過合法註冊之終端機，閱讀應用程式 322 會繼續以解密所取得之第二加密鑰匙 328 對接收到的密文解密，使用者就可以在閱讀應用程式 322 所提供的介面下閱讀解密過後電子書籍。

當閱讀應用程式 322 對解密所取得之電腦辨識碼 330 與目前終端機 106 之電腦辨識碼 318 進行比對後發現比對結果不相同時，代表目前終端機 106 並未經過合法註冊，閱讀應用程式 322 即停止後續動作，也不會如正常情形般以第二加密鑰匙 328 對收到的密文解密，因此使用者也就無法閱讀電子書籍。這種情形會發生的最可能原因，是一個合法使用者於合法註冊的終端機下載電子書籍後，卻將閱讀應用程式 322 連同其購買的電子書籍以及於註冊時所產生終端機加密檔 326 一併拷貝至另一台電腦上，以便給其他電腦上的第三人閱讀，也就是所謂的「合法購買卻非法散佈」。



五、發明說明 (12)

然而，由於本發明之閱讀應用程式 322 對電子書籍解密前，會先對終端機加密檔 326 中所取得的電腦辨識碼 330 與目前解密工作所在電腦之電腦辨識碼 318 進行比對，而取得一個比對的結果。如果目前解密工作所在電腦與註冊當時之終端機是同一電腦，此一比對結果自然會相同，即表示代表目前解密工作所在電腦為經過合法註冊之終端機，電子書籍並未被非法散佈至其他未經合法註冊的電腦中，於是閱讀應用程式 322 會繼續以解密讓使用者可以閱讀解密過後的電子書籍。如果目前解密工作所在電腦與註冊當時之終端機不相同，此一比對結果自然不相同，即表示代表目前解密工作所在電腦並未經過合法註冊，也就是說，電子書籍已經被非法散佈至其他未經合法註冊的電腦中，於是閱讀應用程式 322 會停止解密的步驟，使用者即使取得非法散佈的電子書籍也無法進行解密閱讀。

請參閱圖五，圖五 A 為本發明防盜拷電腦系統在文件索取程序時於伺服器主機端之流程圖，圖五 B 為本發明防盜拷電腦系統在文件索取程序時於終端機之流程圖。將上述文件索取程序以流程圖 500 表示如下列步驟：

步驟 502：開始；

步驟 504：使用者於網路書店中決定購買某一本電子書籍；

步驟 506：伺服器主機 102 處理購買訂單並進行必要的確認及查證；



五、發明說明 (13)

步驟 508：訂單是否通過查證？是，到步驟 512；否，到步驟 510；

步驟 510：拒絕接受此次訂單並立即停止交易；到步驟 540；

步驟 512：於電子文件資料庫 276 中調出購買的電子書籍的明文；

步驟 514：於密碼資料庫 274 中調出使用者專屬之第二加密鑰匙 328；

步驟 516：以此第二加密鑰匙 328 對電子書籍的明文加密以形成相對應之密文；

步驟 518：將密文經由網際網路 104 傳送至終端機 106；

步驟 520：終端機 106 之閱讀應用程式 322 以第一加密鑰匙 324 對終端機加密檔 326 解密；

步驟 522：解密後取得第二加密鑰匙 328 與電腦辨識碼 330；

步驟 524：取得目前工作所在電腦之電腦辨識碼 318；

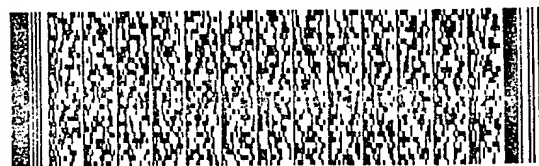
步驟 526：閱讀應用程式 322 對解密所取得之電腦辨識碼 330 與目前電腦之電腦辨識碼 318 進行比對；

步驟 528：比對結果是否相同？是，到步驟 530；否，

步驟 536；

步驟 530：目前終端機 106 已確認經過合法註冊；

步驟 532：閱讀應用程式 322 以第二加密鑰匙 328 對接收到的電子書籍密文解密；



五、發明說明 (14)

步驟 534：使用者可以閱讀解密過後的電子書籍；到
步驟 540；

步驟 536：目前終端機未經過合法註冊；

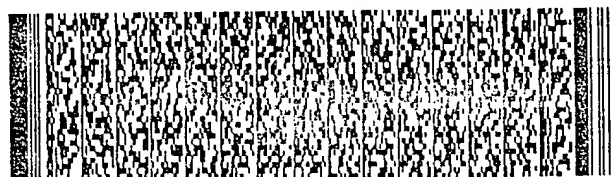
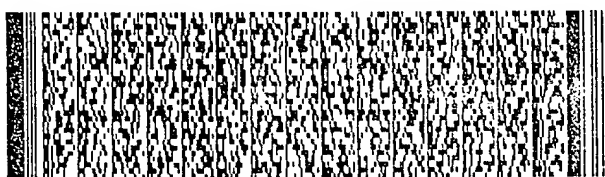
步驟 538：閱讀應用程式 322停止解密動作；

步驟 540：結束。

本發明上述之較佳實施例是以私鑰密碼系統為例加以說明，也就是說對電子書籍加密解密用的是同一把加密鑰匙，除了資料傳輸之雙方外，其他第三人並不知道加密鑰匙的內容為何，因此也稱為對稱型的密碼系統，如美國國家標準局所公佈的 DES演算法，或是 Lai及 Massey所設計的 IDEA演算法，其安全性較強，加解密時運算速度也較快。然而，本發明之電腦系統 100同樣也可採用公開金鑰密碼系統來對電子書籍加密與解密，也就是說每一個使用者會擁有一把可以公佈出來的公開金鑰，與一把自己保留不能洩漏的私有金鑰，當伺服器主機 102之加密模組 250對電子書籍加密時，用的是使用者的公開金鑰，而當閱讀應用程式 322對接收到的電子書籍密文進行解密時，用的是使用者的私有金鑰。

與習知技術相比較，本發明防盜拷電腦系統 100之優點在於：

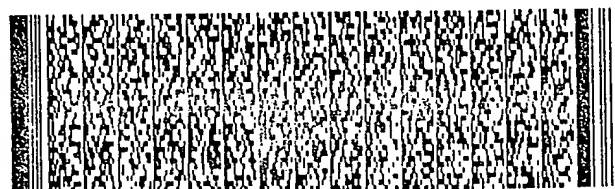
一、不同使用者或終端機所需要的閱讀操作平台都是相同的。由於所有使用者都是經由閱讀應用程式 322與伺



五、發明說明 (15)

伺服器主機 102 進行註冊及文件索取的程序，閱讀應用程式 322 則成為一閱讀操作平台，以提供使用者與伺服器主機 102 溝通的橋樑，閱讀應用程式 322 及其中之第一加密鑰匙 324 都是事先經過編譯完成而可供使用者免費下載或拷貝至任何機器上。由於本發明電腦系統的目的之一在於防止電子書籍推廣時所可能造成的阻卻事由，也就是防止電子書籍的非法散佈，而不在於防止閱讀應用程式 322 本身的散佈，同時由於本發明防止電子書籍非法散佈的機制主要並不在於閱讀應用程式 322 本身，因此，閱讀應用程式 322 經由使用者大量的下載、拷貝或散佈不但不會影響本發明目的，反而有助於推銷電子書籍的概念給使用者，使電子書籍的使用能加速普及。

二、使用者在為其所指定的終端機註冊時，伺服器主機 102 之加密鑰匙產生模組 240 會產生一專屬於使用者的第二加密鑰匙。當使用者購買某一本電子書籍時，加密模組 250 會以此第二加密鑰匙 328 對電子書籍的明文加密以形成相對應之密文，傳送使用者所在之終端機上，而終端機上之閱讀應用程式 322 在確認目前終端機經過合法註冊後，始再以第二加密鑰匙 328 對接收到的電子書籍密文解密。由於某些先前技術對不同使用者購買的電子書籍都以相同的加密鑰匙作加解密，一旦此一加密鑰匙被破解，則所有電子書籍的密文都可以正確被還原成明文；然而本發明針對每一使用者都有專屬的第二加密鑰匙，因此即使某

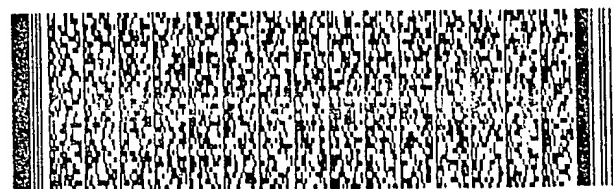
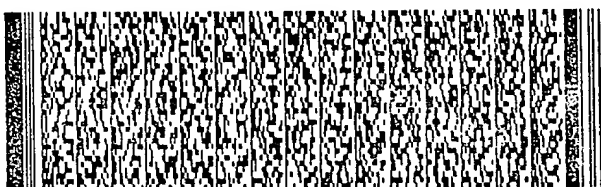


五、發明說明 (16)

一使用者的第二加密鑰匙被破解，仍然無法閱讀其他使用者所購買之電子書籍，因此可提高系統的安全性。

三、終端機加密檔以加密之形式儲存於終端機中，可避免使用者不小心更改其中的內容，也可以減低其他人以非法的方式查看並得知其中的內容。

四、終端機加密檔儲存於終端機，有助於簡化因電腦辨識碼上傳所帶來的隱私權公開時需使用者同意之複雜程序。由於本發明於認證終端機是否經合法註冊所需要的電腦辨識碼，是借用其中中央處理器之辨識碼、硬碟機之辨識碼或是網路卡之辨識碼等為之，而這些辨識碼的資料依法是視為使用者個人隱私資料之一部份，伺服器主機 102 對於使用者所提出任何這類辨識碼之取得都要經過使用者的同意，因此，只要伺服器主機 102 想取得終端機的電腦辨識碼都無法規避使用者同意的程序，於是在認證終端機是否經合法註冊的程序上原本應該會變得較為複雜。然而，依據本發明之設計，當使用者在為其所指定的終端機註冊時，下傳之使用者辨識碼與第二加密鑰匙在解密後，會連同代表該終端機之電腦辨識碼會以第一加密鑰匙加密而產生相對應的終端機加密檔，因此在註冊程序進行過程中，並不需將電腦辨識碼上傳給伺服器主機 102。因此當終端機接收到使用者所購買電子書籍之密文時，其所執行之後續認證程序所需之電腦辨識碼是註冊時就直接儲存於

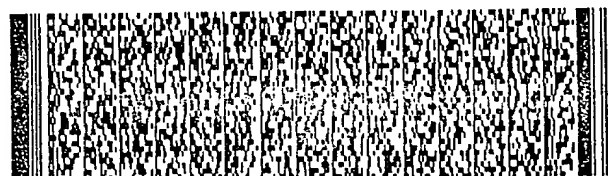
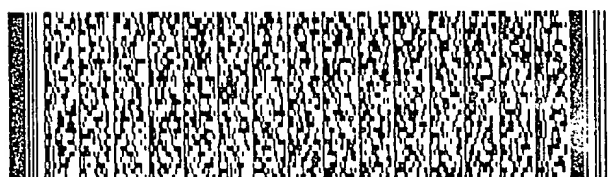


五、發明說明 (17)

終端機中，因此目前工作終端機之電腦辨識碼自然也不必上傳至伺服器主機 102，而可以直接在終端機中進行比較及認證的工作，自然簡化了因電腦辨識碼上傳所會帶來的隱私權公開需要使用者同意之複雜程序及可能的爭議。

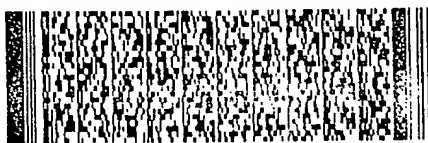
五、利用終端機加密檔 326 中所取得的電腦辨識碼 330 與目前解密工作所在電腦之電腦辨識碼 318 進行比對，可防止「合法購買卻非法散佈」之情事。由於本發明之閱讀應用程式 322 對電子書籍解密前，會先對終端機加密檔 326 中所取得的電腦辨識碼 330 與目前解密工作所在電腦之電腦辨識碼 318 進行比對，以確認目前解密工作所在電腦與註冊當時之終端機是同一電腦，其次再決定並閱讀應用程式 322 是否會繼續進行電子書籍密文的解密工作。因此，即使電子書籍的密文被非法散佈至其他未經合法註冊的電腦中，閱讀應用程式 322 會停止解密的步驟，使非法散佈的電子書籍無法正確解密而無法進行閱讀。

綜上所述，本發明電腦系統提出了一種有效的機制，來防止非經合法註冊之終端機對電子文件之盜拷，因而遏阻「合法購買卻非法散佈」的情形，使得電子書籍的經銷商因可維持合理的利潤而願意投入於書籍電子化買賣的行列當中，因此使得電子書籍之環保性、效率性、傳播性、經濟性等多重優點可為全民所共享。



五、發明說明 (18)

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明專利之涵蓋範圍。



圖式簡單說明

圖式之簡單說明

圖一為本發明可防止電子文件盜拷之電腦系統之示意圖。

圖二為本發明防盜拷電腦系統之伺服器主機的功能方塊圖。

圖三為本發明防盜拷電腦系統之終端機的功能方塊圖

圖四為本發明防盜拷電腦系統於註冊程序時之流程圖。

圖五 A為本發明防盜拷電腦系統在文件索取程序時於伺服器主機端之流程圖。

圖五 B為本發明防盜拷電腦系統在文件索取程序時於用戶終端機之流程圖。

圖示之符號說明

100 防盜拷電腦系統
103 防火牆裝置
106、108、110 終端機

210 介面模組

230 註冊模組

250 加密模組

270 資料庫

274 密碼資料庫

102 伺服器主機

104 網際網路

220 公用程式模組

240 加密鑰匙產生模組

260 交易處理及查證模組

272 用戶資料庫

276 電子文件資料庫



圖式簡單說明

280	控制中心	302	中央處理器
304	硬碟機	306	網路卡
308	鍵盤	310	滑鼠
312	搖桿	314	螢幕
316	印表機		
318	目前工作終端機之電腦辨識碼		
320	記憶體	322	閱讀應用程式
324	第一加密鑰匙	326	終端機加密檔
327	使用者識別碼	328	第二加密鑰匙
330	電腦辨識碼		



六、申請專利範圍

1. 一種使用於一電腦系統中可防止電子文件盜拷之方法，該電腦系統包含有一伺服器主機可經由一網際網路與複數個終端機相連接，每一終端機並具有至少一代表該終端機之辨識碼，一終端機可經由該網際網路向該伺服器主機提出索取一電子文件之要求，該伺服器主機則可將該電子文件之明文經過加密形成相對應之密文，並經由該網際網路傳送至該終端機，以將該密文解密為原來之明文，該方法包含有一註冊程序與一文件索取程序，該註冊程序包含有下列步驟：

使用者載入一閱讀應用程式於一終端機中，該閱讀應用程式並包含一第一加密鑰匙；

使用者利用該閱讀應用程式向該伺服器主機註冊成為一合法之終端機；

該伺服器主機在完成該終端機之合法註冊後，會產生一使用者辨識碼與一使用者專屬之第二加密鑰匙，該使用者辨識碼與該第二加密鑰匙並會經過加密後傳送至該合法註冊之終端機；以及

該終端機之閱讀應用程式並會進一步將接收到之使用者辨識碼與第二加密鑰匙連同代表該終端機之辨識碼一併加密以形成一終端機加密檔，以儲存於該合法註冊之終端機中；

該文件索取程序包含有下列步驟：

當一終端機向該伺服器主機提出索取一電子文件之要求時，該伺服器主機則會將該電子文件之明文經過該第二



六、申請專利範圍

加密鑰匙之加密而形成相對應之密文，並將該密文經由該網際網路傳送至該終端機；

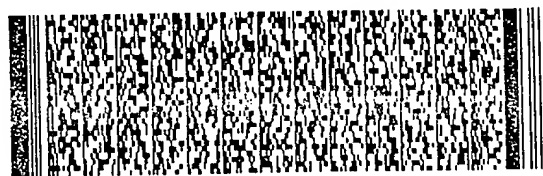
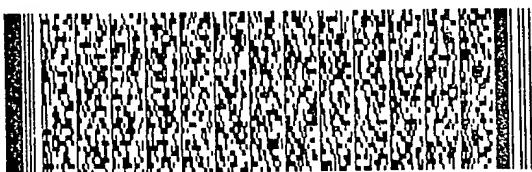
當該終端機之閱讀應用程式接收到該密文時，會先以該第一加密鑰匙對該終端機加密檔解密，並取得其中之第二加密鑰匙與該終端機之辨識碼；以及

當該閱讀應用程式比較所取得之終端機辨識碼與目前終端機之辨識碼為相同時，即以該第二加密鑰匙對該接收到的密文解密，否則即停止後續之解密動作，以防止非合法之終端機對該電子文件之盜拷。

○ 如申請專利範圍第 1 項之方法，其中該終端機另包含一中央處理器、一硬碟機以及一網路卡，而該終端機之辨識碼可為該中央處理器之辨識碼、該硬碟機之辨識碼或是該網路卡之辨識碼。

3. 如申請專利範圍第 1 項之方法，其中該伺服器主機中包含有一用戶資料庫，以記錄經由該註冊程序所註冊之所有合法的使用者及其終端機之辨識碼。

4. 如申請專利範圍第 3 項之方法，其中該伺服器主機中包含有一加密鑰匙產生模組，該加密鑰匙產生模組會對該用戶資料庫中所註冊之不同使用者各自產生該使用者專屬之第二加密鑰匙。



六、申請專利範圍

5. 如申請專利範圍第4項之方法，其中該伺服器主機中包含有一密碼資料庫，該密碼資料庫中儲存有所有經過註冊之使用者資料及其專屬之第二加密鑰匙。

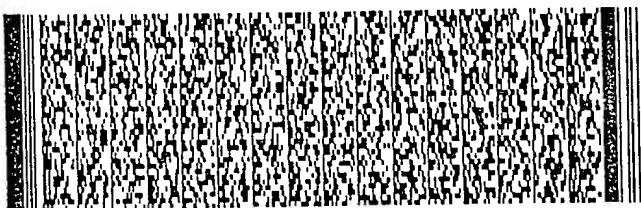
6. 如申請專利範圍第1項之方法，其中該伺服器主機中包含有一加密模組，當該終端機完成合法註冊後，該加密模組會對該第二加密鑰匙與該使用者辨識碼加密後並傳送至該合法註冊之終端機。

7. 如申請專利範圍第6項之方法，其中該伺服器主機中包含有一電子文件資料庫以儲存複數個電子文件之明文資料，以及一控制中心，用來控制該伺服器主機之操作。

8. 如申請專利範圍第7項之方法，其中當該伺服器主機收到索取該電子文件之要求時，該控制中心會至該電子文件資料庫調出該電子文件之明文資料，而該加密模組會以該第二加密鑰匙對該電子文件之明文加密，以形成相對應之密文。

9. 如申請專利範圍第1項之方法，其中該第一加密鑰匙與該第二加密鑰匙皆為具有一二八位元之數位序列。

10. 如申請專利範圍第1項之方法，其中該伺服器主機中包含有一公用程式模組，以存放該閱讀應用程式並供使用



六、申請專利範圍

者下載至該終端機中儲存使用。

11. 一種可防止電子文件盜拷之電腦系統，該電腦系統包含有一伺服器主機可經由一網際網路以與複數個終端機相連接，每一終端機並具有至少一代表該終端機之辨識碼，一終端機可經由該網際網路向該伺服器主機提出索取一電子文件之要求，該伺服器主機則可將該電子文件之明文經過加密形成相對應之密文，並經由該網際網路傳送至該終端機，以將該密文解密為原來之明文，該伺服器主機包含有：

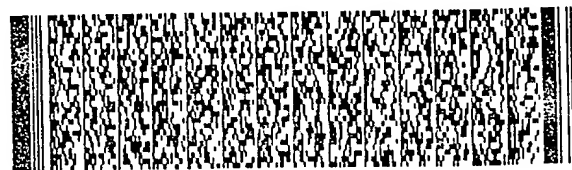
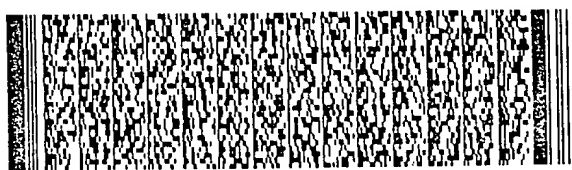
一公用程式模組，以存放包含一第一加密鑰匙之閱讀應用程式，該閱讀應用程式並可供使用者下載至該終端機中儲存使用；

一註冊模組，當使用者利用該終端機之閱讀應用程式向該伺服器主機註冊時，該註冊模組會產生一使用者辨識碼並將該終端機註冊為一合法之終端機；

一加密鑰匙產生模組，用來產生一使用者專屬之第二加密鑰匙；以及

一加密模組，用來將該使用者辨識碼與該第二加密鑰匙加密，並傳送至該合法註冊之終端機中；

其中該終端機之閱讀應用程式並會進一步將接收到之使用者辨識碼與第二加密鑰匙連同代表該終端機之電腦辨識碼一併加密以形成一終端機加密檔，以儲存於該合法註冊之終端機中，而當一終端機向該伺服器主機提出索取一



六、申請專利範圍

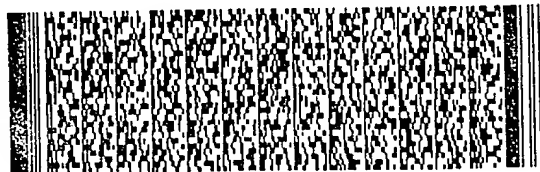
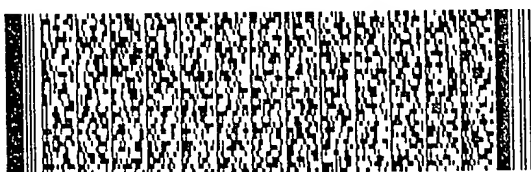
電子文件之要求時，該加密模組會以該第二加密鑰匙將該電子文件之明文加密而形成相對應之密文，並將該密文經由該網際網路傳送至該終端機，當該終端機之閱讀應用程式接收到該密文時，會先以該第一加密鑰匙對該終端機加密檔解密，並取得其中之第二加密鑰匙與該辨識碼，而當該閱讀應用程式比較所取得之辨識碼與目前終端機之辨識碼為相同時，即以該第二加密鑰匙對該接收到的密文解密，否則即停止後續之解密動作，以防止非合法之終端機對該電子文件之盜拷。

2. 如申請專利範圍第 11 項之電腦系統，其中該終端機另包含一中央處理器、一硬碟機以及一網路卡，而該終端機之辨識碼可為該中央處理器之辨識碼、該硬碟機之辨識碼或是該網路卡之辨識碼。

13. 如申請專利範圍第 11 項之電腦系統，其中該伺服器主機中包含有一用戶資料庫，以記錄所有合法註冊的使用者及其終端機之辨識碼。

14. 如申請專利範圍第 11 項之電腦系統，其中該伺服器主機中包含有一密碼資料庫，該密碼資料庫中儲存有所有經過註冊之使用者資料及其專屬之第二加密鑰匙。

15. 如申請專利範圍第 11 項之電腦系統，其中該伺服器主

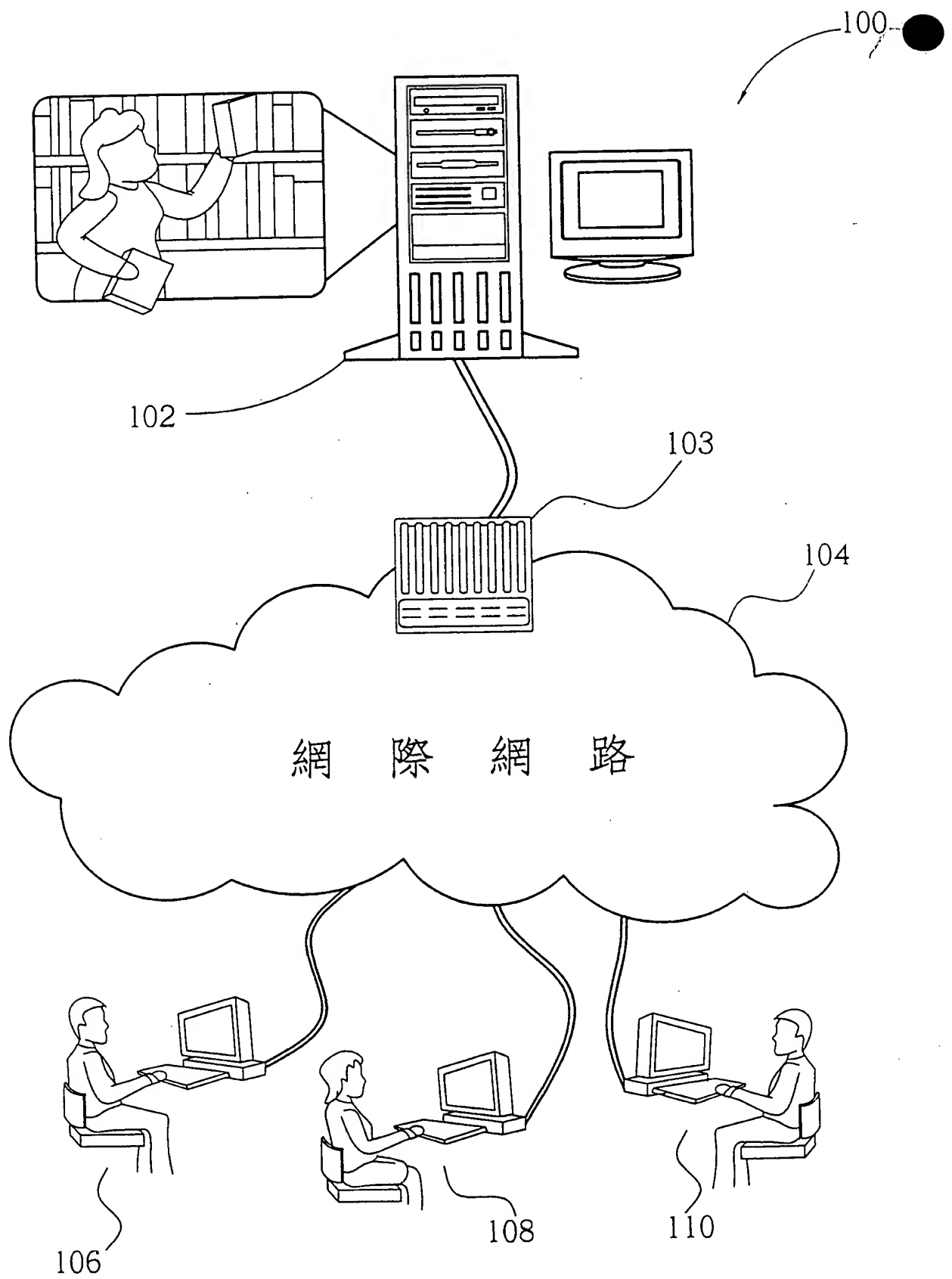


六、申請專利範圍

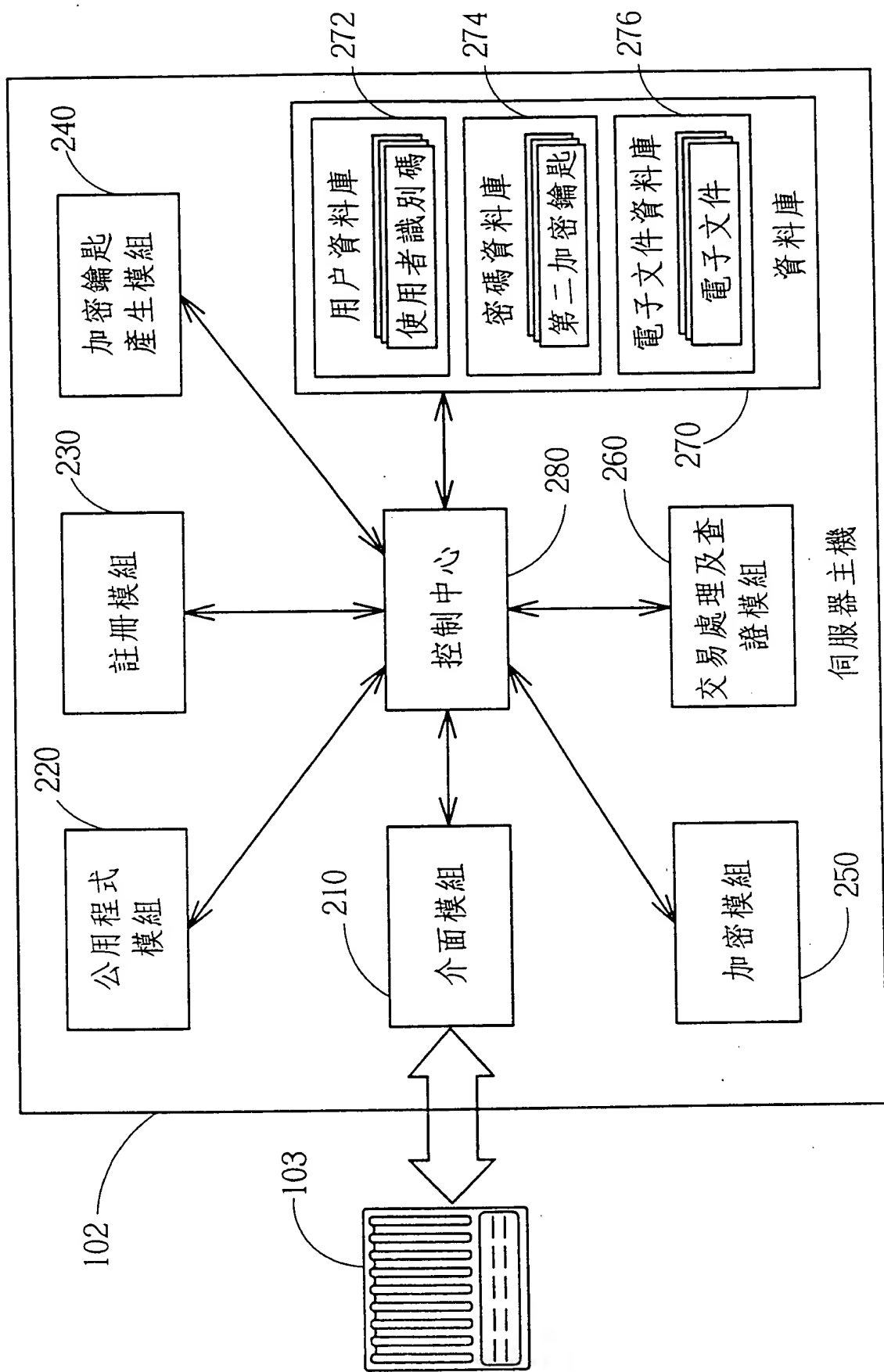
機中包含有一電子文件資料庫以儲存複數個電子文件之明文資料，以及一控制中心，用來控制該伺服器主機之操作。

16. 如申請專利範圍第15項之電腦系統，其中當該伺服器主機收到索取該電子文件之要求時，該控制中心會至該電子文件資料庫調出該電子文件之明文資料，而該加密模組會以該第二加密鑰匙對該電子文件之明文加密，以形成相對應之密文。

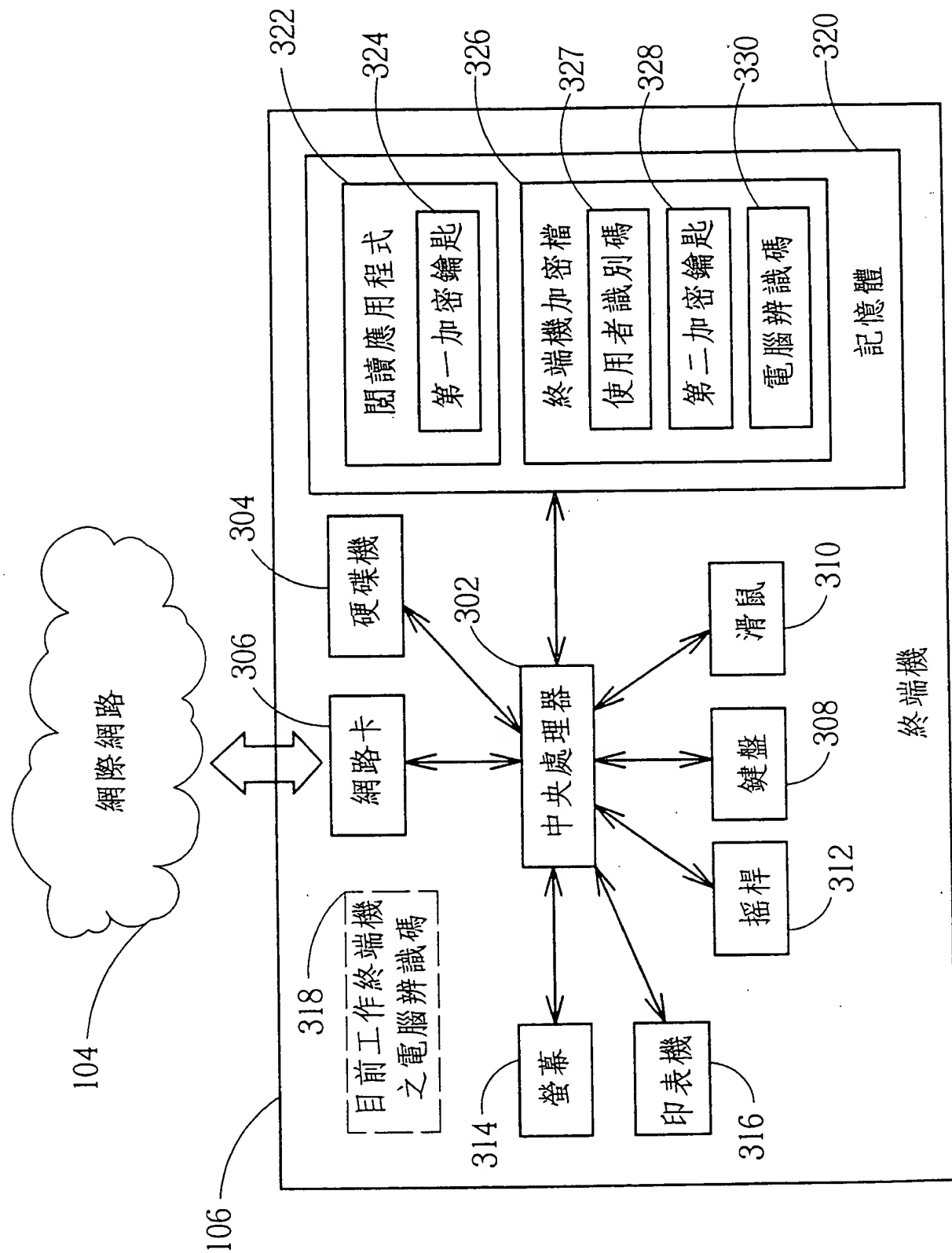
17. 如申請專利範圍第11項之電腦系統，其中該第一加密鑰匙與該第二加密鑰匙皆為具有一二八位元之數位序列。



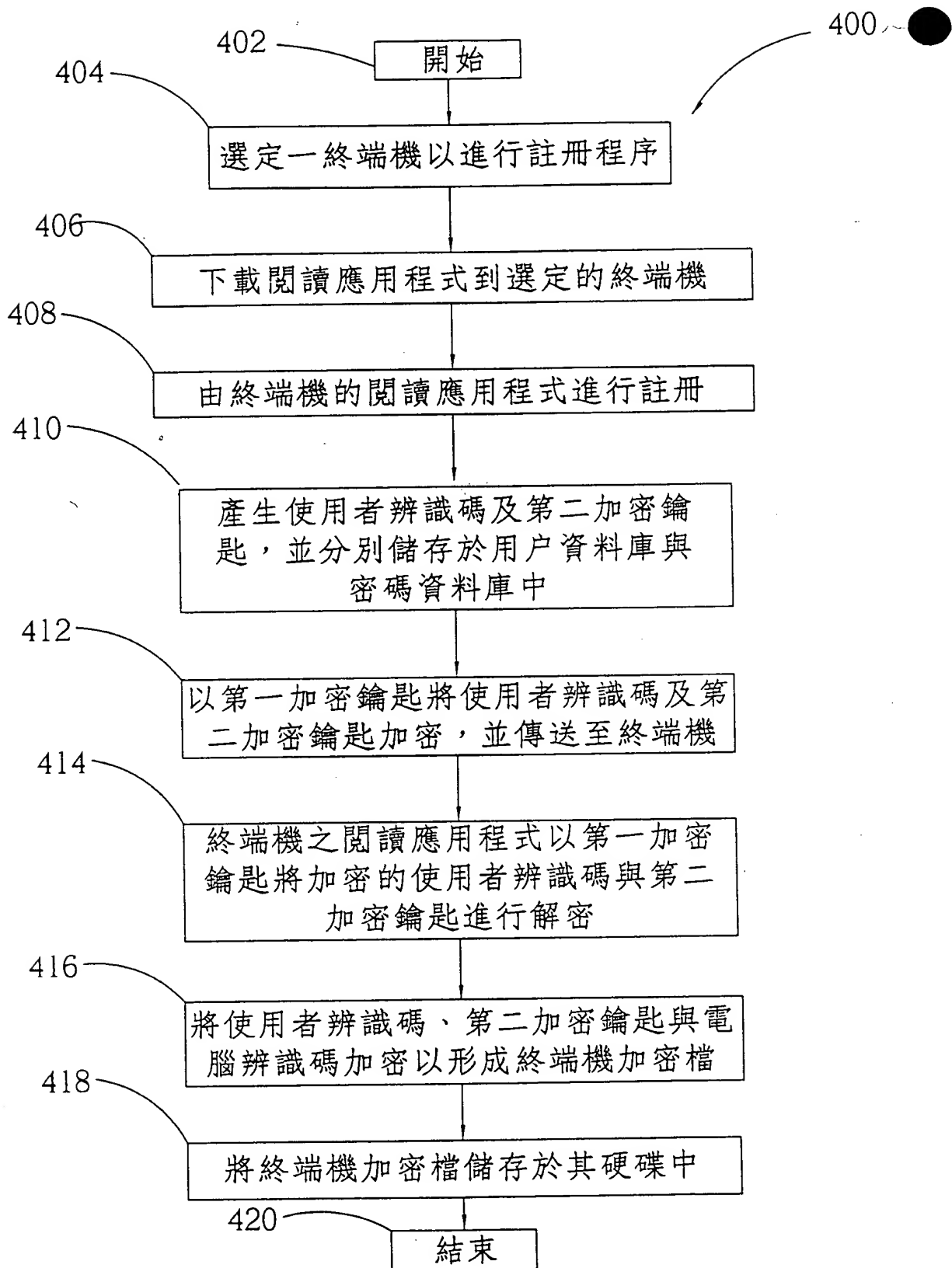
圖一



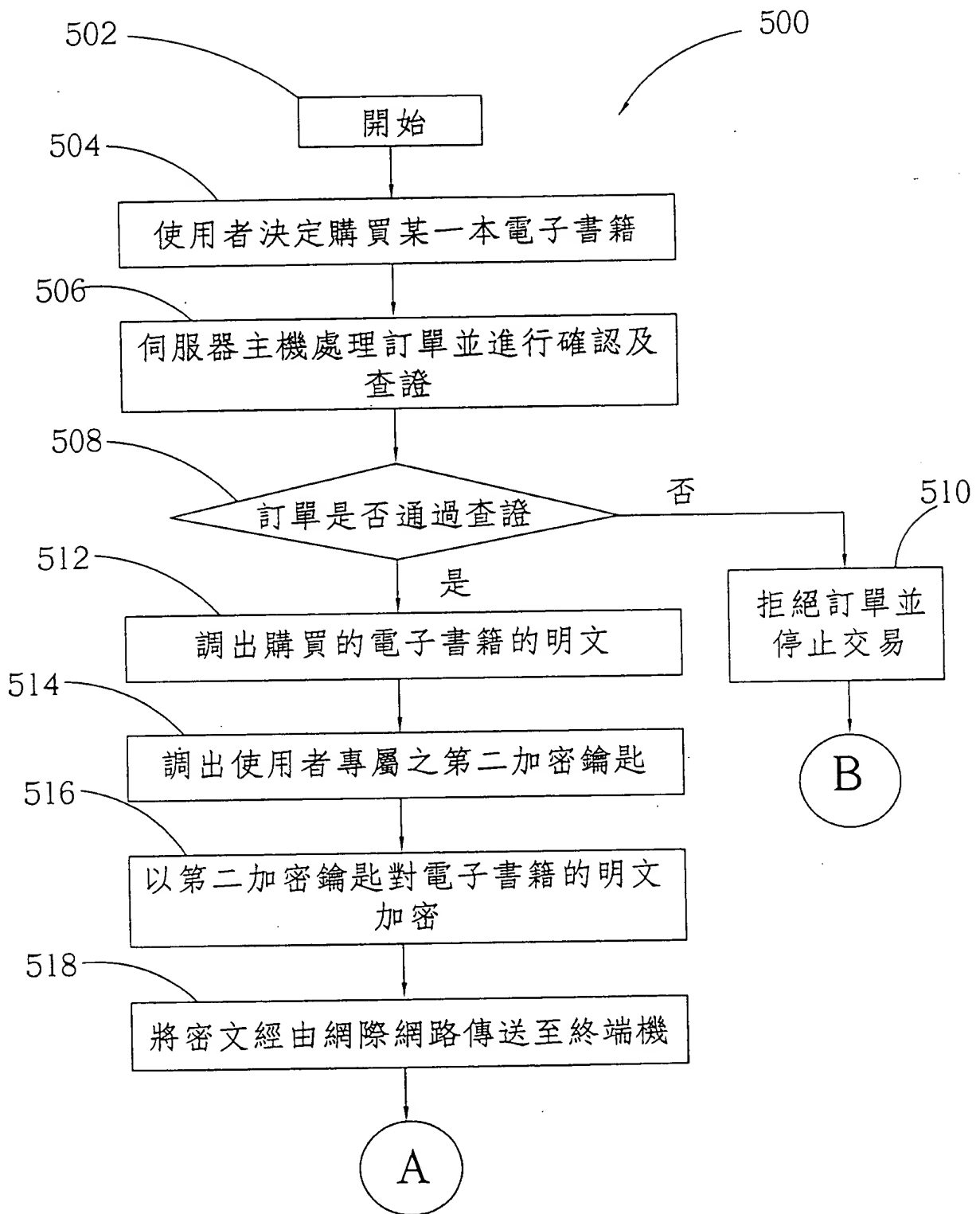
圖二



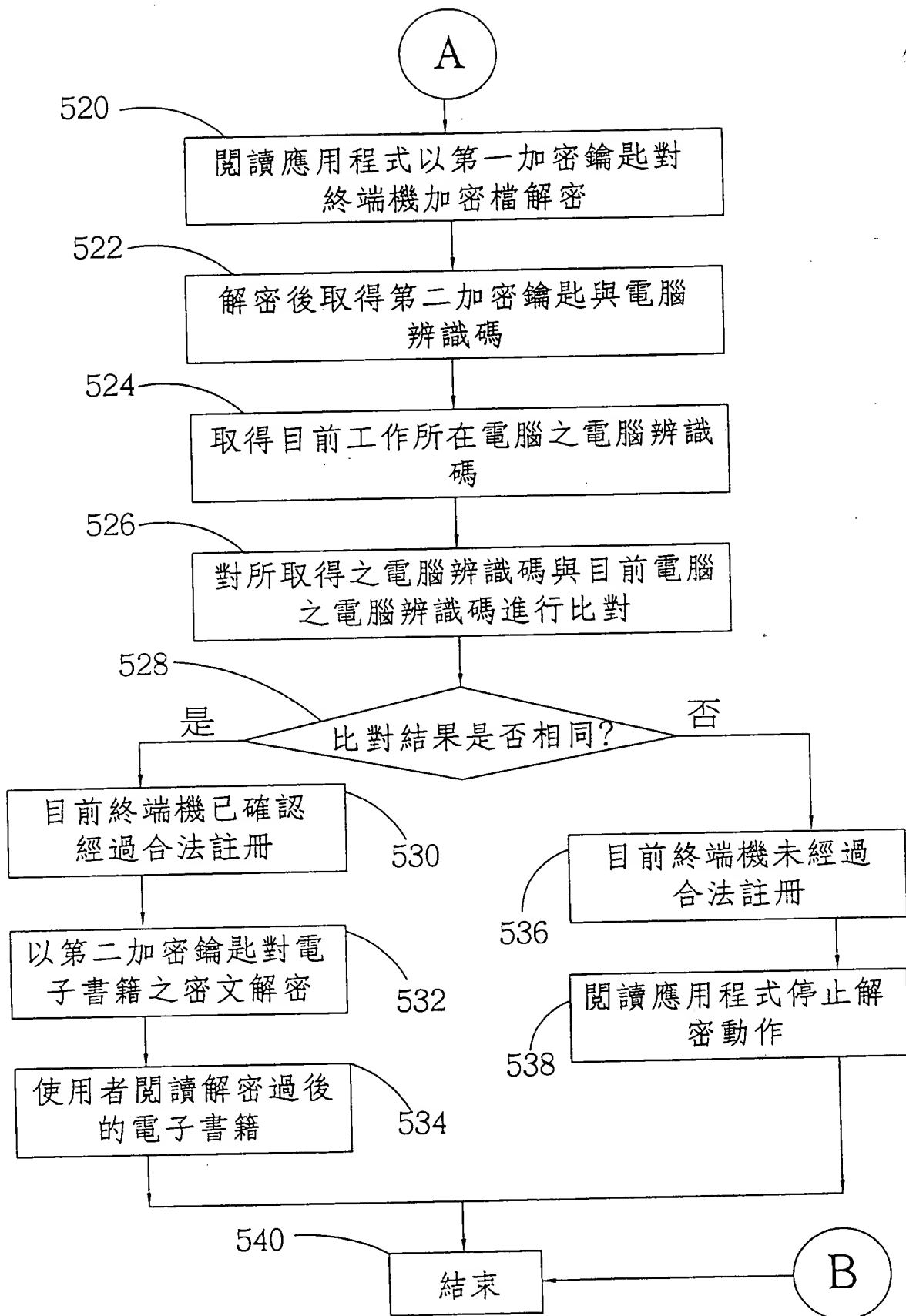
圖三



圖四

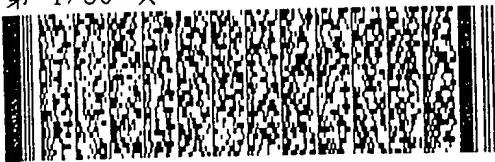


圖五A

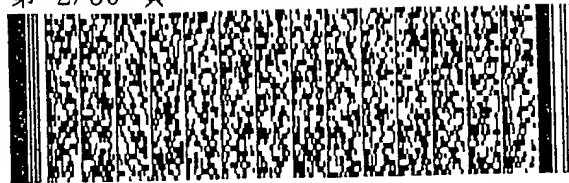


圖五B

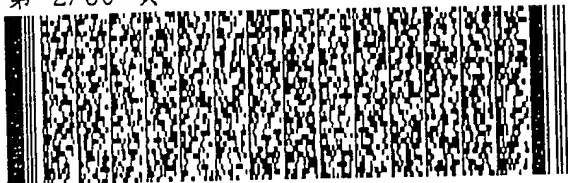
第 1/30 頁



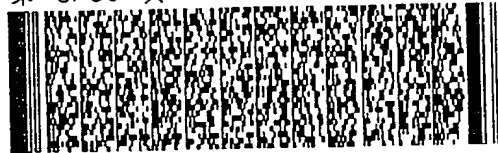
第 2/30 頁



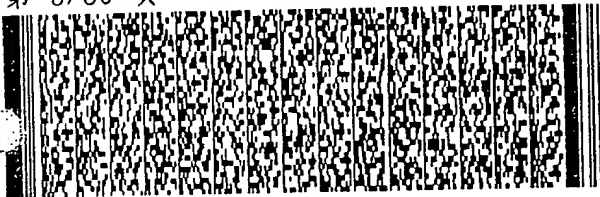
第 2/30 頁



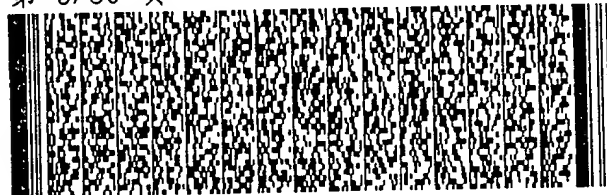
第 3/30 頁



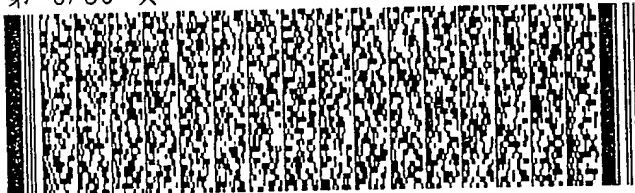
第 5/30 頁



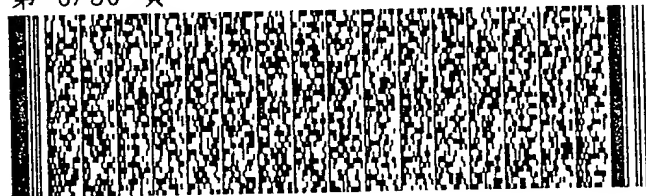
第 5/30 頁



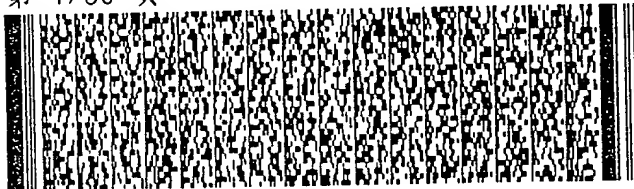
第 6/30 頁



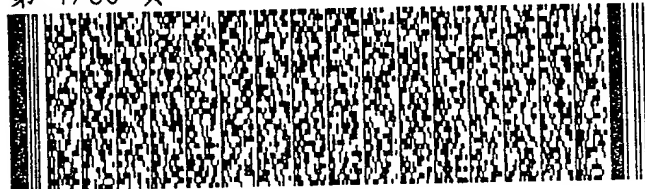
第 6/30 頁



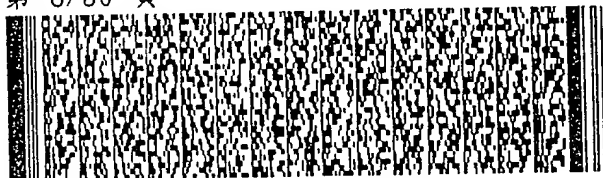
第 7/30 頁



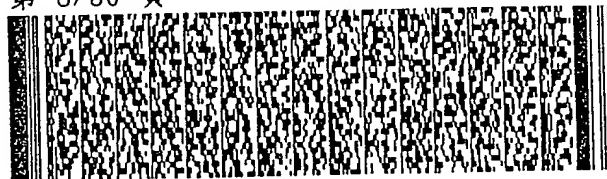
第 7/30 頁



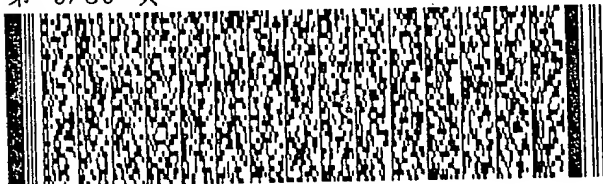
第 8/30 頁



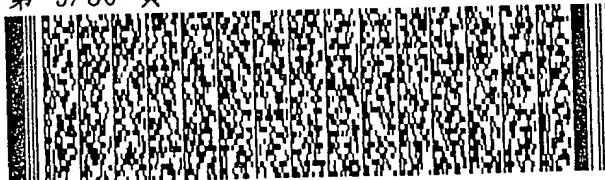
第 8/30 頁



第 9/30 頁



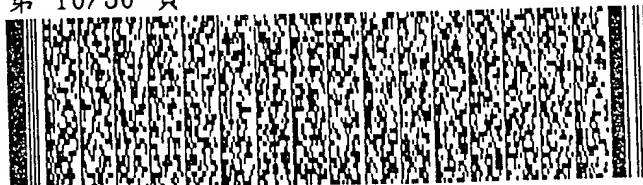
第 9/30 頁



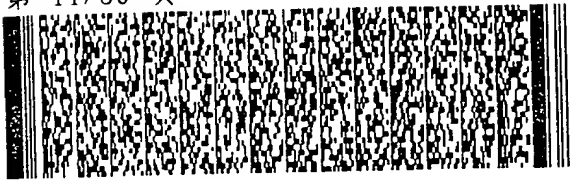
第 10/30 頁



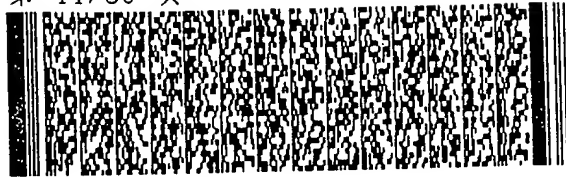
第 10/30 頁



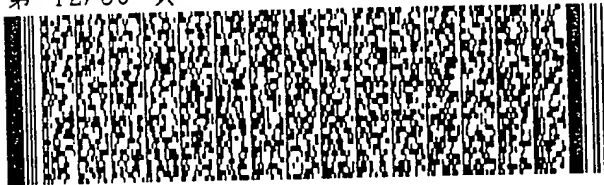
第 11/30 頁



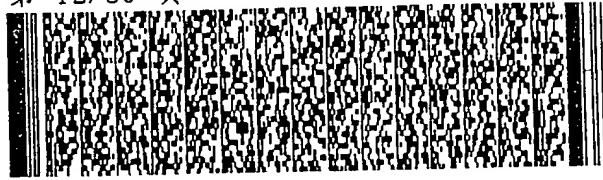
第 11/30 頁



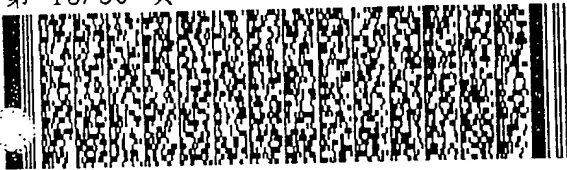
第 12/30 頁



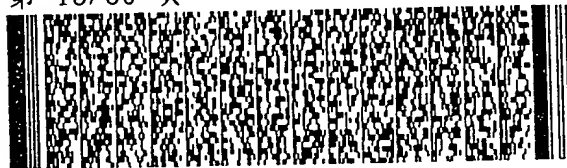
第 12/30 頁



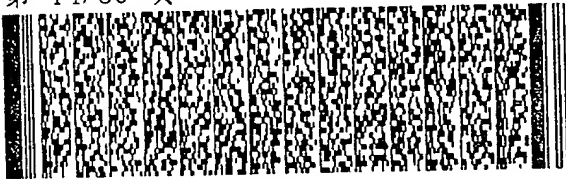
第 13/30 頁



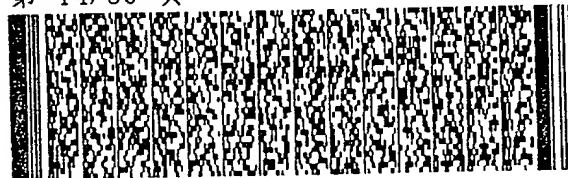
第 13/30 頁



第 14/30 頁



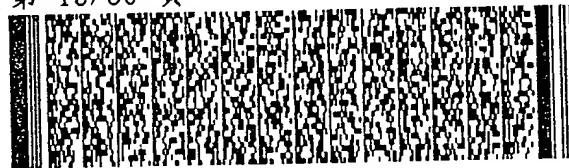
第 14/30 頁



第 15/30 頁



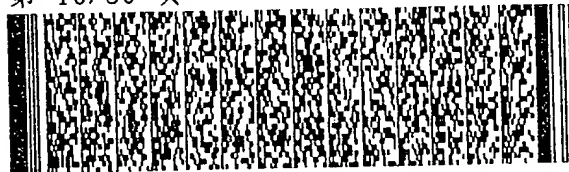
第 15/30 頁



第 16/30 頁



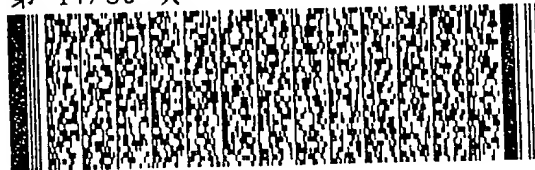
第 16/30 頁



第 17/30 頁



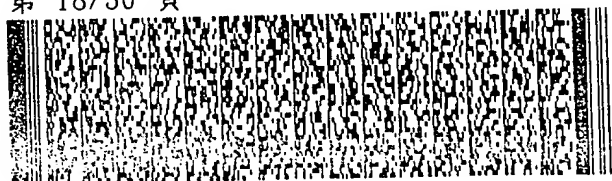
第 17/30 頁



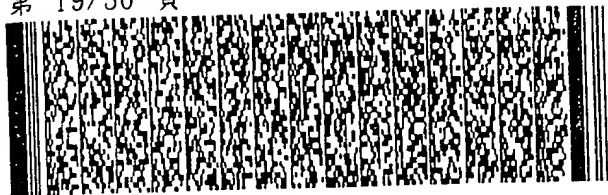
第 18/30 頁



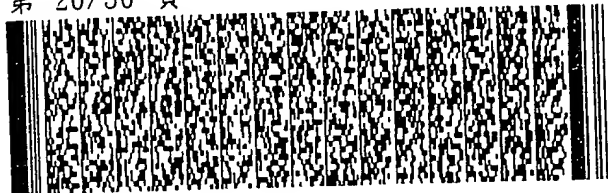
第 18/30 頁



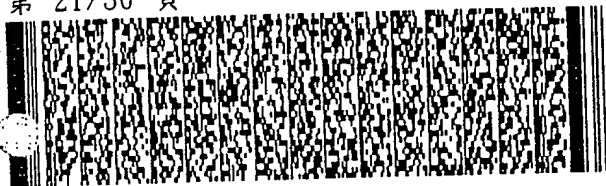
第 19/30 頁



第 20/30 頁



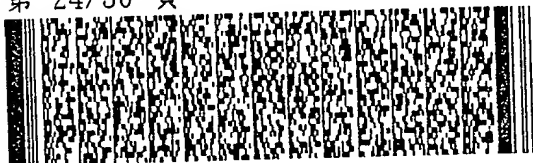
第 21/30 頁



第 22/30 頁



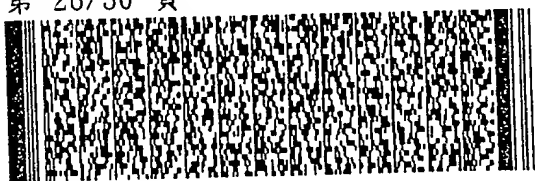
第 24/30 頁



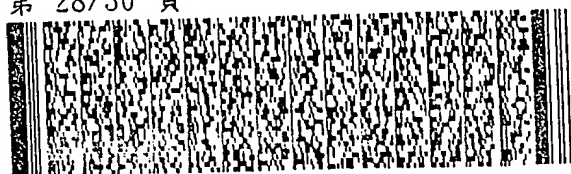
第 25/30 頁



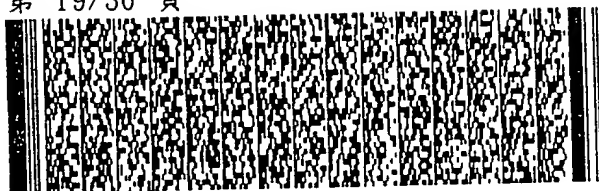
第 26/30 頁



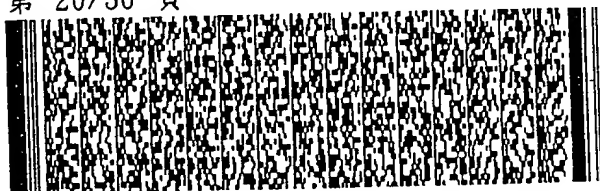
第 28/30 頁



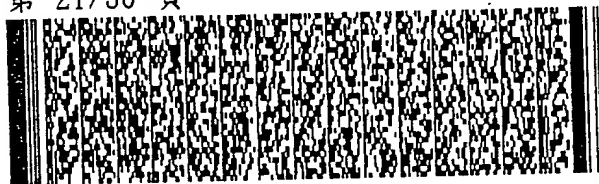
第 19/30 頁



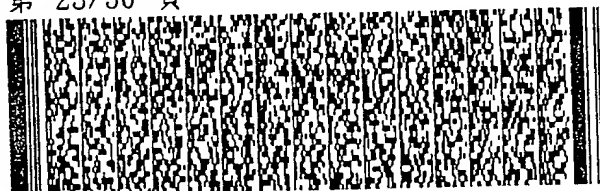
第 20/30 頁



第 21/30 頁



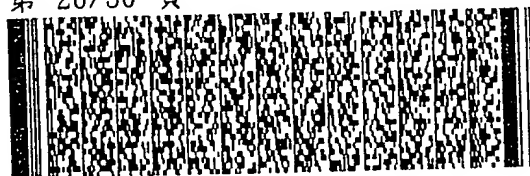
第 23/30 頁



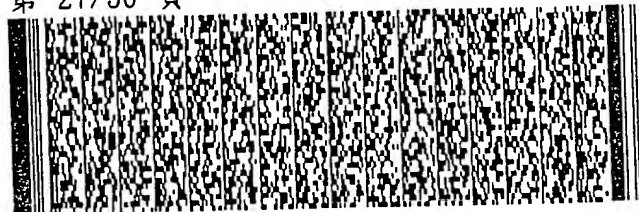
第 25/30 頁



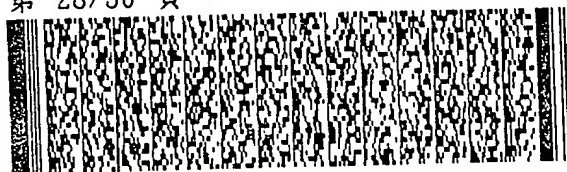
第 26/30 頁



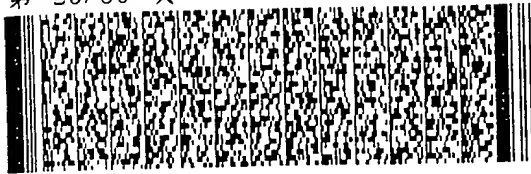
第 27/30 頁



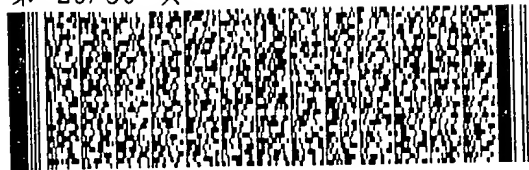
第 28/30 頁



第 29/30 頁



第 29/30 頁



第 30/30 頁

